CLAIMS

1. Apparatus adapted to communicate via a network, comprising:

a firewall (124), for identifying those packets associated with inappropriate activity; and

at least one user discernable indicator (126) associated with said firewall, for contemporaneously indicating that a number of packets associated with said inappropriate activity have exceeded a threshold level.

2. The apparatus of claim 1, wherein said inappropriate activity is determined using a plurality of rules divided into classes indicative of levels of inappropriateness.

3. The apparatus of claim 1, wherein said apparatus comprises at least one of a modem, a router and a bridge (202).

4. The apparatus of claim 1, wherein said indicator comprises at least one visual indicator.

5. The apparatus of claim 4, wherein said at least one visual indicator comprises a light emitting device proximate to said apparatus.

6. The apparatus of claim 4, wherein said at least one visual indicator comprises a highlighted icon displayed on a computing device (260).

7. A method, comprising:

examining data traffic to determine whether at least one of a plurality of rules has been violated, said rules defining indicators of inappropriate communication activity; and

in the case of a rule of at least a first class of the plurality of rules being violated, filtering said data traffic violating said first class rule and triggering a user discernable indicator.

8. The method of claim 7, further comprising:

determining if a first threshold level of rule violation has been exceeded prior to filtering said data traffic.

9. The method of claim 7, further comprising:

determining if a first threshold level of rule violation has been exceeded prior to triggering the user discernable indicator.

10. The method of claim 7, wherein in the case of a rule of a second class being violated, filtering said data traffic violating said second class rule and triggering the user discernable indicator.

11. The method of claim 10, further comprising:

determining if a second threshold level of rule violation has been exceeded prior to filtering said data traffic.

12. The method of claim 10, further comprising:

determining if a second threshold level of rule violation has been exceeded prior to triggering the user discernable indicator.

13. The method of claim 7, wherein a case of a rule of a third class being violated, filtering said data traffic violating said third class rule; and

triggering the user discernable indicator.

14. The method of claim 13, further comprising:

determining if a third threshold level of rule violation has been exceeded prior to filtering said data traffic.

15. The method of claim 13, further comprising:

determining if a third threshold level of rule violation has been exceeded prior to triggering the user discernable indicator.

16. A cable modem (202), comprising:

downstream processing circuitry (210);

upstream processing circuitry (212);

a controller (204) in communication with said downstream circuits, upstream circuitry, and a memory (108); and

a firewall program (124) having associated with it a set of rules, said firewall program resident in said memory and executable by said controller to cause examining data of packets from said downstream and upstream circuitry such that inappropriate activity above a threshold level results in the triggering for at least one visual indicator (126) positioned proximate said cable modem, said at least one visual indicator for discernable viewing by a user.

17. The cable modem of claim 16, wherein said at least one visual indicator comprises at least one light emitting diode (LED).

18. The cable modem of claim 16, wherein said at least one visual indicator comprises a first LED for signifying a filtering event and a second LED for signifying filtering data packets deemed pernicious in said set of rules.

19. The apparatus of claim 16, wherein said at least one visual indicator comprises a highlighted icon displayed on a computer device (260).